SECURE SYSTEM FIRMWARE USING INTERRUPT GENERATION ON ATTEMPTS TO MODIFY SHADOW RAM ATTRIBUTES

ABSTRACT

A system, method and software that secures system firmware located in shadow RAM from unauthorized tampering. The present invention adds protection, either as a whole, or to individual portions of shadow RAM, using a configuration register in a memory controller (or other chip containing shadow RAM attribute control), or an external trapping chip, that traps accesses to a register or registers normally used to enable reading, writing and/or caching of the shadow RAM and generates an interrupt. Only resetting of the trapping chip unlocks the shadow RAM and allows modifications to reading, writing and/or caching of the shadow RAM area. Since trusted code gains control after reset, malicious or run-away programs cannot gain control while the shadow RAM is vulnerable. The entire shadow RAM area or individual shadow RAM areas may be controlled. The present invention permits use of code in the shadow RAM without fear of its alteration, raising reliability from run-away applications or malicious attack.